REMARKS

The Office is thanked for the careful review of the subject application.

Claims 24-46 are pending in the present application. Claims 24, 28, 32, 36, and 40 are independent claims. In the subject paper, no claims have been amended, added, or canceled. The Applicant believes that the present application is now in condition for allowance, which prompt and favorable action is respectfully requested.

Allowable Subject Matter

Initially, the Applicant appreciates the Office's withdrawal of the rejection of claims 28-35 under 35 U.S.C. § 101, the withdrawal of the rejection of claims 24-45 under 35 U.S.C. § 103 (a), and the indication that claims 24-46 would be allowed if the 35 U.S.C. § 112, 1st paragraph rejection based on an alleged enablement deficiency is overcome.

35 U.S.C. § 112, 1st Paragraph - Enablement

Claims 24-46 were rejected under 35 U.S.C. § 112, 1st paragraph as allegedly failing the enablement requirement. The Applicant respectfully traverses this rejection.

The Office assumes that the claimed "credential server" serves *multiple* devices, which implies that each of the multiple devices has its own master credential (*e.g., see* Pages 2-3 of the 12/4/2008 Office Action). Based on this assumption and its implications, the Office's position appears to be that it is unclear how the claimed "credential server" knows which master credential to use in generating the application credential if it only knows the application identifier.

The Applicant notes that the claims are not directed to ***how*** the credential server associates the master credentials of multiple devices. Because this aspect is not claimed, it does not necessarily matter if specific examples regarding how this aspect could be performed are not included in the Specification. Accordingly, the issue is simply whether the ***claims*** are ***enabled***. Pursuant to MPEP 2164.01, the test for enablement is as follows:

> Any analysis of whether a particular claim is supported by the disclosure in an application requires a determination of whether that disclosure, when filed, contained sufficient information regarding the subject matter of the claims as *to enable one skilled in the pertinent art to make and use the claimed invention*. The standard for determining whether the specification meets the enablement requirement was cast in the Supreme Court decision of *Mineral Separation v. Hyde,* 242 U.S. 261, 270 (1916) *which postured the question: is the experimentation needed to practice the invention undue or unreasonable?* That standard is still the one to be applied. *In re Wands*, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988). ***Accordingly, even though the statute does not use the term "undue experimentation," it has been interpreted to require that the claimed invention be enabled so that any person skilled in the art can make and use the invention without undue experimentation.*** *In re Wands*, 858 F.2d at 737, 8 USPQ2d at 1404 (Fed. Cir. 1988). See also *United States v. Telectronics, Inc.,* 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988) ("The test of enablement is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation."). ***A patent need not teach, and preferably omits, what is well known in the art.*** *In re Buchner*, 929 F.2d 660, 661, 18 USPQ2d 1331, 1332 (Fed. Cir. 1991); *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1384, 231 USPQ 81, 94 (Fed. Cir. 1986), *cert. denied*, 480 U.S. 947 (1987); and *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1463, 221 USPQ 481, 489 (Fed. Cir. 1984). (*Emphasis in bold has been added by Applicant)*

Additionally, the Applicant directs the Office to the Specification at Paragraph [0029], which states the following:

> [0029] The device includes a copy of a master credential that was installed in the device during manufacture, or by using some other secure procedure that protects the master credential from public disclosure. The master credential is also known to a credential server.

First, turning back to the Office's arguments that the claims are not enabled due to a lack of clarity related to how the master credential is loaded for *multiple* devices, even assuming the Office's position is correct (which the Applicant does not agree with), the Applicant does not believe that this issue supports an enablement rejection of the Applicant's claims. Specifically, the claims do not require multiple devices and, as described in paragraph 29 provided above, *one device's master credential stored at the credential server is sufficient to satisfy the enablement requirement*. The Applicant respectfully submits that the Office has not raised any enablement issues based on the actual claim language and in particular to the embodiment discussed above.

As previously noted, the only enablement issue appears to be based on an issue raised by the Office regarding multiple master credentials stored at the credential server.

Second, assuming that master credentials for different devices are stored at the credential server, the Applicant respectfully submits that the credential server could simply generate a "server credential using the application identifier and a master credential" for each master credential stored and then authenticating the application "if the server credential and the application credential match," as claimed. In other words, there is no requirement that the credential server knows which master credential belongs to a particular device, because the credential server can simply check the stored master credentials to determine if any of the master credentials function to authenticate the application. The Applicant respectfully submits that nothing in the claim language limits the credential server to only operating once.

Third, the Applicant directs the Office to the Specification at Paragraph [0029], which was previously cited. The device includes a copy of a master credential that was installed in the device during manufacture, or by using some other secure procedure that protects the master credential from public disclosure. The master credential is also known to a credential server.

The association of the master credential to the device can be accomplished by various techniques which would be understood by one of ordinary skill in the art and would not require *undue experimentation*. For example, the credential server could simply associate the master credential with its associated device using a lookup table which is well known in the art.

Once again, the Applicant notes these implementation details are not required by the claim. The Applicant also respectfully submits that the claims also do not preclude any additional implementation aspects. Regardless, these issues do not impact enablement of the pending claims.

For the reasons given above, the Applicant respectfully submits that one of ordinary skill in the art could obtain the claimed invention without undue experimentation based on the Specification as originally filed, and as such the claims satisfy the enablement requirement of 35 U.S.C. § 112, 1st paragraph. As such, the Applicant respectfully requests that the Office withdraw this rejection.

Reconsideration and issuance of the present application is respectfully requested.

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: March 3, 2009

By: /Fariba Yadegar-Bandari/

Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502